

SMITH NORMAL FORMS OF INCIDENCE MATRICES

PETER SIN

ABSTRACT. A brief introduction is given to the topic of Smith normal forms of incidence matrices. A general discussion of techniques is illustrated by some classical examples. Some recent advances are described and the limits of our current understanding are indicated.

1. INTRODUCTION

An incidence matrix is a matrix A of zeros and ones which encodes a relation between two finite sets X and Y . Related elements are said to be *incident*. The rows of the incidence matrix A are indexed by the elements of X , ordered in some way, and the columns are indexed by Y . The (x, y) entry is 1 if x and y are incident and zero otherwise. Many of the incidence relations we shall consider will be special cases or variations of the following basic examples.

Example 1.1. Let S be a set of size n and for two fixed numbers k and j with $0 \leq k \leq j \leq n$ let X be the set of all subsets of S of size k and Y the set of subsets of S of size j . The most obvious incidence relation is set inclusion but, more generally, for each $t \leq k$ we have a natural incidence relation in which elements of X and Y to be incident if their intersection has size t .

Example 1.2. The example above has a “ q -analog” in which X and Y are the sets of k -dimensional and j -dimensional subspaces of an n -dimensional vector space over a finite field \mathbf{F}_q , with incidence being inclusion, or more generally, specified by the dimensions of the subspace intersections. It is common in this context to use the terminology of projective geometry, referring to 1-dimensional subspaces as points, 2-dimensional subspaces as lines, etc. of the projective space $PG(n-1, q)$.

Further examples of incidence relations abound from graph theory and design theory, and we will discuss both general classes and specific examples.

We may view A as having entries over any commutative ring with 1 but in this paper we shall always assume that the entries are integers, which is the most general case, in the sense that many results for other rings such as fields can be deduced from results over \mathbf{Z} .

An incidence matrix translates an incidence relation, with no loss of information, into linear algebra. Thus, we are led inescapably to the study of its algebraic invariants. In the case where $X = Y$, we could consider the spectrum of the square matrix A , or its rational canonical form. For the general case, where A is not necessarily square, the fundamental invariant is the *Smith normal form* of A , whose definition we now recall. A square integer matrix is *unimodular* if it is invertible in the ring of integer matrices, which is the same as saying that its determinant is ± 1 . Two integer matrices A and B are *equivalent over \mathbf{Z}* if

This work was partially supported by a grant from the Simons Foundation (#204181 to Peter Sin).

there exist unimodular matrices P and Q such that $B = PAQ$. It is a standard theorem that every integer matrix is equivalent to one of the form

$$(1) \quad PAQ = \begin{pmatrix} s_1 & 0 & 0 & 0 & \dots \\ 0 & \ddots & 0 & 0 & \dots \\ 0 & 0 & s_r & 0 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

where r is the rank of A and $s_i | s_{i+1}$ for $i = 1, \dots, r-1$. The entries s_i are uniquely determined up to signs and the matrix is called the Smith normal form (SNF) of A . (The form is named after H. J. S. Smith, who also showed [34] that $s_i = d_i/d_{i-1}$, where $d_0 = 1$ and d_i for $i \geq 1$ is the greatest common divisor of the $(i \times i)$ minors of A).

The SNF is a natural choice of invariant for an incidence relation as it does not depend on an arbitrary ordering of the sets. In other words, it is the same for all possible incidence matrices of the relation.

Of course, it is well known how to bring an integer matrix to Smith normal form by applying row and column operations corresponding to left and right multiplications by unimodular matrices in a systematic way, based on the euclidean algorithm. However, we are interested in solving this problem not for one incidence matrix at a time but for parametrized families of such matrices. The object is to describe the SNFs (or equivalent forms) uniformly as functions of the parameters. Such computations could be expected to provide insight into the mathematical structure of the incidence relations.

The purpose of this article is to provide an introduction to the topic of computing the SNFs of families of incidence matrices. Thanks to the existence of a readable and thorough survey [41] on the SNF of incidence matrices of designs, and the related question of their p -ranks, much of the history and literature has been covered, and we can concentrate instead on elucidating some of the algebraic techniques that have been introduced, and on describing some recent results and open questions.

2. GENERALITIES ON SMITH NORMAL FORM

Let R be a principal ideal domain and A an $m \times n$ matrix with entries in R . In our examples, R will be either \mathbf{Z} or the localization at a nonzero prime of the ring of integers in a number field. The definition of SNF can, *mutatis mutandis*, be extended to R . If we view A as the matrix of the homomorphism $\eta : R^m \rightarrow R^n$ by matrix multiplication on the right, then the SNF is one of several ways of describing the cyclic decomposition of the *Smith module* $G(\eta) = R^n / \text{Im}(\eta)$, namely in its *invariant factor form*¹.

While the term “SNF” is traditional and is a useful label, it is really the Smith module $G(\eta)$ which is at the center of interest. A matrix equivalent to A which has nonzero entries only on the diagonal is called a *diagonal form* of A . Since a diagonal form describes $G(\eta)$ up to isomorphism, it also counts as a valid solution to the “SNF problem”. Another alternative description of $G(\eta)$ is the *elementary divisor form*, which can be thought of as the set of p -local SNFs for all primes p dividing the order of torsion subgroup of $G(\eta)$.

¹Some minor differences in terminology are found in the literature. Many authors do not allow 1 as an invariant factor or elementary divisor, which is quite reasonable from the module-theoretic viewpoint. However, in studying matrices or maps it is often more convenient to think of the invariant factors as the list of the r nonzero entries s_i of the SNF, including those equal to 1. Then, for $1 \leq i \leq r$, the exact power of a prime π dividing s_i is called the i -th π -elementary divisor. This is the convention we shall adopt.

Different problems lend themselves to different decompositions of $G(\eta)$, so it is best to be flexible about the exact formulation of results. For instance, in the case of inclusion of k -subsets in j -subsets of an n -set, the most natural diagonal form turns out to have binomial coefficients as entries, with multiplicities equal to differences of binomial coefficients. In this case, to give elementary divisors would involve consideration of the exact power to which each prime divides a binomial coefficient, which, although it is well known, would make the statements much more complicated. It would be even more challenging to give a uniform description of the invariant factor form, but the point is that the extra difficulty comes from the arithmetic of binomial coefficients and not from the incidence relation. In the case of inclusion of points in linear subspaces of a projective space, it will be seen that if p is the underlying characteristic, the most natural decomposition of the torsion subgroup of $G(\eta)$ is as the direct sum of a p -group, described by a p -local SNF, and a cyclic group of order prime to p .

Suppose \mathcal{B} is a basis of R^m and \mathcal{C} is a basis of R^n such that the matrix of η in these bases is diagonal. Then we shall call \mathcal{B} a *left SNF basis* and \mathcal{C} a *right SNF basis*. In terms of a matrix equation

$$PAQ = D,$$

with P and Q unimodular (i.e. invertible over R) and D in diagonal form, \mathcal{B} corresponds to the rows of P and \mathcal{C} to the rows of Q^{-1} .

2.1. Local SNFs. On occasion, we shall be forced to consider certain extensions of the PID R . For example we may wish to adjoin roots of unity to \mathbf{Z} . In general this may take us out of the realm of PIDs into Dedekind domains, but since the SNF problem can be solved one prime at a time we can localize, bringing us back to PIDs, in fact to discrete valuation rings. Therefore, we shall consider an extension $R \subset R'$ of PIDs and compare $G(\eta)$, the cokernel of $\eta : M \rightarrow N$ with the cokernel $G(1 \otimes \eta)$ of the induced map $1 \otimes \eta : R' \otimes_R M \rightarrow R' \otimes_R N$. Since tensoring R -modules with R' is a right exact functor, we have

$$(2) \quad G(1 \otimes_R \eta) \cong R' \otimes_R G(\eta).$$

In the simplest situation, where the prime $p \in R$ is unramified in R' , and π is a prime of R' above p , the multiplicity of p^i as an elementary divisor of η is equal to the multiplicity of π^i as an elementary divisor of $1 \otimes_R \eta$.

Let R be a discrete valuation ring of characteristic zero with fraction field K , maximal ideal (π) and residue field $k = R/(\pi)$ of characteristic $p > 0$. Given a homomorphism

$$(3) \quad \eta : M \rightarrow N$$

of free R -modules of finite rank, we define

$$(4) \quad M_i = M_i(\eta) = \{m \in M \mid \eta(m) \in \pi^i N\},$$

and

$$(5) \quad N_i = N_i(\eta) = \{\pi^{-i} \eta(m) \mid m \in M_i\}.$$

We have

$$(6) \quad M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

and

$$(7) \quad \text{Im } \eta = N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

Let \overline{M}_i and \overline{N}_i be the images of M_i and N_i in $\overline{M} = M/\pi M$ and $\overline{N} = N/\pi N$ respectively.

There exist ℓ, ℓ' such that $\overline{M}_i = \overline{\ker \eta}$ for $i \geq \ell$ and N_j is equal to the purification of $\text{Im } \eta$ for $j \geq \ell'$.

Let $e_i(\eta)$ denote the multiplicity of π^i as an elementary divisor of η . Then, as is easily seen from considering the SNF of η , we have

$$(8) \quad e_i(\eta) = \dim(\overline{M}_i / \overline{M}_{i+1}) = \dim(\overline{N}_i / \overline{N}_{i-1}).$$

(We set $N_{-1} = 0$.) Left and right SNF bases can be constructed from the modules M_i and N_j as follows. Choose bases \overline{B}_i for the \overline{M}_i that are “nested”, by which is meant that $\overline{B}_\ell \subseteq \overline{B}_{\ell-1} \subseteq \cdots \subseteq \overline{B}_0$. First we let $\overline{D}_\ell = \overline{B}_\ell$ and for $i = 0, \dots, \ell - 1$ we set $\overline{D}_i = \overline{B}_i \setminus \overline{B}_{i+1}$. Let D_ℓ be a basis of $\ker \eta$ which maps onto \overline{D}_ℓ and for $i = 0, \dots, \ell - 1$, let $D_i \subseteq M_i$ be a set which maps bijectively onto \overline{D}_i . Then it is easily verified that $B = \bigcup_{j=0}^\ell D_j$ is a left SNF basis for η . Similarly, a right SNF basis can be constructed by lifting nested bases of the \overline{N}_j .

As observed in [8] these notions are of importance when we wish to compare the SNF of a product AB of two matrices with those of A and B . Of course, it is easy to see that $s_i(A)$ and $s_i(B)$ divide $s_i(AB)$ but little more can be said in general except in trivial cases such as when the Smith modules are finite groups with coprime orders. As a simple example, let

$$(9) \quad A = \begin{pmatrix} 1 & 0 \\ -p & p^2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} p & 0 \\ 1 & p \end{pmatrix}.$$

Then A and B each have elementary divisors 1 and p^2 , while AB has elementary divisors p and p^3 .

Suppose that n is the number of columns of A and the number of rows of B , and suppose that R^n has a basis which is *simultaneously* a right SNF basis for A and a left SNF basis for B . Then we have unimodular matrices P, Q and S such that

$$PAQ = D, \quad Q^{-1}BS = D',$$

with D and D' in diagonal form.

Hence $P(AB)S = DD'$ and we have multiplicativity of the diagonal forms.

The following result (based on an argument in [8]) shows how the rare phenomenon of multiplicativity of diagonal forms may arise from certain group actions.

Proposition 2.1. *Let K be the fraction field of R . Suppose that we have an abelian group G of order prime to p , R -free RG -modules X, Y and Z , and RG -module homomorphisms $\alpha : X \rightarrow Y$ and $\beta : Y \rightarrow Z$. Assume further that the action of KG on $K \otimes_R Y$ is multiplicity-free, i.e. no two simple composition factors are isomorphic. Then Y has a basis which is simultaneously a right SNF basis for α and a left SNF basis for β .*

Proof. Let ξ be a primitive $|G|$ -th root of unity in an algebraic closure of K . Then since (π) is unramified in $R[\xi]$, the π -elementary divisors of the induced maps $1 \otimes \alpha$, $1 \otimes \beta$ and $1 \otimes \beta \circ \alpha$ are the same as those for α , β and $\beta \circ \alpha$. Also the multiplicity-free hypothesis is still valid if we extend the ring to $R[\xi]$. Therefore, we may assume that $R = R[\xi]$. In this case, we have a decomposition of $K \otimes_R Y$ as a direct sum of one-dimensional components K_χ , where each χ is a character of G . The element

$$h_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

is a projection onto K_χ which lies in the center of RG , and $\sum_{\chi \in \text{Hom}(G, R^\times)} h_\chi = 1$. Therefore, we also have the decomposition $Y = \bigoplus_\chi R_\chi$, where $R_\chi = Y \cap K_\chi$. Let v_χ be a generator of

R_χ , so that the v_χ form a basis \mathcal{B} . We claim that \mathcal{B} is simultaneously a left SNF basis for β and a right SNF basis for α . The images \bar{v}_χ of the v_χ form a basis $\bar{\mathcal{B}}$ of \bar{Y} . The multiplicity-free condition means that for every submodule of \bar{Y} there is a subset of $\bar{\mathcal{B}}$ which is a basis. Thus, in the construction of a left SNF basis B described in §2.1 (with $\eta = \beta$, $M = Y$ and $N = Z$) we can take the nested bases \bar{B}_i to be subsets of $\bar{\mathcal{B}}$. Hence, if $x \in D_i \subset M_i$ then the image of x in \bar{M} is some \bar{v}_χ . It follows that $h_\chi x = uv_\chi$, for some unit $u \in R$, so in fact $v_\chi \in M_i$. If we replace x by v_χ , in B , the resulting set is again a left SNF basis for β . This means that the set of all the v_χ is a left SNF basis for β . An identical argument about the construction of a right SNF basis from the N_j shows that the set of all v_χ is also a right SNF basis for α . \square

A characterization of the SNF by some simple properties is given in [27]. Other general properties of the Smith group and some applications are discussed in [28] and [29].

3. THE SNF PROBLEM FOR INCIDENCE MATRICES

In applying the general theory of the previous section to incidence problems we start with $M = \mathbf{Z}^X$ and $N = \mathbf{Z}^Y$ and $\eta : M \rightarrow N$, sending $x \in X$ to the sum of all elements of Y incident with x . If there is an action of a group G on X and Y that preserves the incidence relation, then M and N are permutation $\mathbf{Z}G$ -modules and η is a $\mathbf{Z}G$ -module homomorphism. For example in Example 1.1, the symmetric group S_n acts, and in Example 1.2 we may take $G = \mathrm{GL}(n, q)$. The spaces \mathbf{Q}^X and \mathbf{Q}^Y have inner products for which X and Y are orthonormal bases, and then M and N are unimodular lattices. If $\eta^* : N \rightarrow M$ is the transpose of η , sending $y \in Y$ to the sum of elements of X incident with it, then we have

$$\langle x, \eta^*(y) \rangle = \langle \eta(x), y \rangle.$$

If we work over a discrete valuation ring R , then the modules M_i and N_i of §2.1 are RG -submodules of M and N . Further, \bar{M} , \bar{M}_i , \bar{N} , \bar{N}_i are $\bar{R}G$ -modules. In some cases, one can find a very direct connection between the RG -submodule structure of these modules and the SNF, using (8).

Many families of incidence relations are encompassed by Examples 1.1 and 1.2, and most of the SNF problems are unsolved. The complete solutions in some important cases and progress in other cases will form a large part of our discussion. A particular family may be an example of a general combinatorial structure such as a strongly regular graph, design or difference set, so our next task is to examine properties of these general structures that are relevant to the SNF problem.

3.1. Graphs. In the case where the incidence relation is between sets X and Y which are equal, or are in bijection in some prescribed way, the incidence matrix A can be regarded as the adjacency matrix of a directed graph, which is simple if no element is related to itself.

In addition to the SNF one can also consider the eigenvalues of A . This applies to some subcases of Examples 1.1 and 1.2, such as when $X = Y$ is the set of k -subsets of an n -set, with disjointness as the incidence, which defines the *Kneser graph* $K(n, k)$, or when $X = Y$ is the set of lines in $PG(3, q)$ with the relation of skewness. The latter example, to which we shall return later, also defines the noncollinearity graph of a hyperbolic quadric in $PG(5, q)$, by the Klein correspondence. At the most general level, there is no close relationship between the

eigenvalues and invariant factors of a square integral matrix, as illustrated by the matrices

$$(10) \quad A_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

whose invariant factors are respectively $(2, 2, 2)$, $(1, 2, 4)$ and $(1, 1, 8)$.

One general observation is the following [10].

Lemma 3.1. *Let A be a square integral matrix with integral eigenvalue a of (geometric) multiplicity m . Then the number of invariant factors of A divisible by a is at least m .*

Let Γ be a regular graph of degree k on v vertices. Then Γ is a *strongly regular graph* (SRG) if, for any pair of vertices, the number of common neighbors depends only on whether the vertices are adjacent or not. If the number of common neighbors for pairs of adjacent vertices is λ and the number for pairs of nonadjacent vertices is μ , then we say that Γ is an SRG with parameters (v, k, λ, μ) . We refer to [10] for properties and many examples of SRGs. An SRG has of course the all-one vector $\mathbf{1}$ as an eigenvector (with eigenvalue k). The orthogonal complement of $\mathbf{1}$ (in the \mathbf{Q} -inner product space with the vertices as orthonormal basis) is the direct sum of eigenspaces for two distinct integral eigenvalues r and s , called the restricted eigenvalues.

The following [10, p.174] gives quite strong information about the p -elementary divisors of an SRG for $p \nmid v$.

Proposition 3.2. *Let A be the adjacency matrix of an SRG with parameters (v, k, λ, μ) and restricted eigenvalues r and s . Let p be a prime and assume that $p \nmid v$, $p^a \parallel k$, $p^b \parallel s$, $p^c \parallel r$, with $a \geq b + c$. Let e_i denote the multiplicity of p^i as an elementary divisor of A . Then $e_i = 0$ for $\min(b, c) < i < \max(b, c)$ and $b + c < i < a$ and $i > a$. Moreover, $e_{b+c-i} = e_i$ for $0 \leq i < \min(b, c)$.*

Of the two examples mentioned above, the noncollinearity graph of the Klein quadric is always an SRG while the Kneser graphs never are.

3.2. Abelian Cayley graphs and difference sets. Suppose a (multiplicative) abelian group G acts regularly on X , preserving an incidence relation $I \subseteq X \times X$. Then by identifying G with X , we have a translation-invariant relation on G . Such relations are uniquely determined by the subset $E = \{e \in G \mid (1, e) \in I\}$, since $(g, h) \in I$ if and only if $g^{-1}h \in E$. The relation can be viewed as adjacency in the Cayley graph of G with respect to the connecting set E . Let A be the adjacency matrix with respect to some fixed order.

Let $C = (\chi(g))$ denote the character table of G , with rows indexed by the set G^\vee of irreducible complex characters of G and the columns indexed by the elements of G , in the same order as for A and $\overline{C} = (\chi(g^{-1}))$.

Then, as first observed in [25], we have

$$(11) \quad \frac{1}{|G|} \overline{C} A C^t = \text{diag}(\chi(E))_{\chi \in G^\vee}.$$

The significance of this equation is twofold. First, the orthogonality relations $\frac{1}{|G|} \overline{C} C^t = I$ show that the $\chi(E)$ are the eigenvalues of A . Secondly, if p is any prime that does not divide $|G|$, we can read the equation as an equivalence over the ring $R = \mathbf{Z}_p[\xi]$, where \mathbf{Z}_p is the ring of p -adic integers and ξ is a primitive $|G|$ -th root of unity. Since p is unramified in R , we see that the exact powers of p dividing the $\chi(E)$ in R are precisely the p -elementary divisors of A .

Here, the general theory ends and the known methods for computing these valuations depend very much on the prime and the relation in question.

Example 3.3. Let S be a set of size mn partitioned into m subsets of size n . Let X be the set of *transversals*, that is, subsets of S of size m that contain one element from each part. Two transversals are incident if and only if they are disjoint. Thus the incidence matrix A is $n^m \times n^m$. Let Z_n be a cyclic group of order n written multiplicatively. We can identify X with the elements of the group $G = (Z_n)^m$ and observe that the regular action of G on itself by multiplication preserves incidence. The set of elements incident with 1_G is $E = \{(a_1, \dots, a_m) \in G \mid a_i \neq 1 \forall i\}$. Let A be the incidence matrix, for some fixed ordering of G . We will apply the equation (11) first to compute the spectrum of A and then to obtain the SNF. First we see from (11) that A is similar to $\text{diag}(\chi(E))_\chi$. The irreducible characters of G are of the form $\chi = (\lambda_1, \dots, \lambda_m)$, where λ_i is an irreducible character of Z_n . Then starting from the fact that

$$\sum_{z \in Z_n \setminus \{1\}} \lambda_i(z) = \begin{cases} -1, & \text{if } \lambda_i \text{ is not principal,} \\ n-1, & \text{if } \lambda_i \text{ is principal,} \end{cases}$$

it follows that $\chi(E) = (-1)^{m-r}(n-1)^r$, where r is the number of i such that λ_i is principal. Also, one sees that the multiplicity of $(-1)^{m-r}(n-1)^r$ as an eigenvalue is the number of characters χ that have exactly r principal components, which is $\binom{m}{r}(n-1)^{m-r}$, since once the r principal components are fixed, there are $n-1$ choices for nonprincipal characters in each of the remaining $m-r$ components. Thus we know that the determinant of A is, up to sign, a power of $(n-1)$ and the SNF involves only primes p dividing $n-1$. If p is such a prime, then in particular $p \nmid |G|$ and we can view (11) as expressing equivalence of matrices over a suitable p -local ring. We may conclude that in a suitable ordering of the characters, $\text{diag}(\chi(E))_\chi$ is actually the SNF of A . The matrix A in this example is the association matrix for the maximal distance in the *Hamming association scheme* $H(m, n)$. (For background on association schemes, see [9].) The eigenvalues of all association matrices for $H(m, n)$ are known [14], but the SNFs of these matrices do not seem to be known. This example was studied in [5], where the SNF was computed for small examples and conjectured in general.

Cayley Graphs can be derived from *difference sets*. An *abelian difference set* is a subset B in an abelian group G such that for some natural number λ each nontrivial element $g \in G$ has the form $g = x^{-1}y$ for precisely λ pairs (x, y) of elements in B . If we take G as the set of points and the translates gB as the set of blocks, the incidence structure obtained has the structure of a *symmetric design* (cf. [23]). Since $gB = g'B$ only for $g = g'$, we can also identify the set of blocks with G , and then we have a G -invariant relation on G of the kind described above, hence a Cayley graph, with $E = B$.

Example 3.4. Let $d \geq 3$ and let q be a power of a prime p . The Singer difference set is a difference set L_0 in $\mathbf{F}_{q^d}^*/\mathbf{F}_q^*$, consisting of those cosets of \mathbf{F}_q^* whose elements y satisfy $\text{Tr}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(y) = 0$. Each character χ of $\mathbf{F}_{q^d}^*/\mathbf{F}_q^*$ is of the form $\omega^{d(q-1)}$, where ω is a generator of the character group of $\mathbf{F}_{q^d}^*$. The *Gauss sum* over \mathbf{F}_{q^d} with respect to the multiplicative character χ and the additive character $y \mapsto \xi^{\text{Tr}_{q^d/p}(y)}$, where ξ is a primitive p -th root of unity is defined as

$$g(\chi) = \sum_{y \in \mathbf{F}_{q^d}^*} \chi(y) \xi^{\text{Tr}_{q^d/p}(y)}.$$

Evaluation of this Gauss sum ([42]; see also [3, p.400]) yields

$$g(\chi) = q\chi(L_0).$$

The \mathfrak{p} -adic valuation of this Gauss sum is determined by a classical theorem of Stickelberger. Computation of the SNF is then a matter of determining the \mathfrak{p} valuation of ω^d in terms of d and counting the d 's for a given valuation. In this way, a new proof of the p -rank was given in [15]. R. Liebler also took this approach towards computing the SNF in unpublished work.

The incidence relation for Singer difference sets can also be interpreted as the incidence of points and hyperplanes in $PG(n, q)$, $n \geq 2$, and so it is both a special case of Example 1.2 and a generalization of the point-line incidence of the projective planes $PG(2, q)$, for which the SNF was computed in [22]. This point-hyperplane incidence for general n but prime fields only was studied by Black and List, who determined the SNF in [6]. Their method was different from the general Cayley graph approach outlined above; instead they viewed the incidence matrix as the so-called rational character table of an elementary abelian group and made a reduction by tensor factorization to the case of a cyclic group of prime order. For the case of arbitrary finite fields, the SNF of the point-hyperplane incidence was first computed using the modular representation theory of $GL(n+1, q)$.

Let $q = p^t$. Let d_λ be the coefficient of z^λ in $(\sum_{j=0}^{p-1} z^j)^{n+1}$. Explicitly,

$$(12) \quad d_\lambda = \sum_{k=0}^{\lfloor \lambda/p \rfloor} (-1)^k \binom{n+1}{k} \binom{n+\lambda-kp}{n}.$$

Define the matrix $M = (m_{i,j})$ ($1 \leq i, j \leq n$) with entries in $\mathbf{Z}[z]$ by $m_{i,j} = d_{pj-i} z^{pj-i}$ and let $a_r = a_{r,t}$ ($0 \leq r \leq t(n-1)$) be the coefficient of $z^{r(p-1)}$ in $\text{trace}(M^t)$.

Theorem 3.5. *The Smith group of the incidence matrix of points and hyperplanes of $PG(n, q)$ has cyclic factors of the following orders and multiplicities:*

- (1) $\frac{(q^n-1)}{(q-1)}$ with multiplicity 1.
- (2) p^r with multiplicity a_r , $0 \leq r \leq (n-1)t$.

It is worth mentioning some representation-theoretic perspectives of this result. The group $G = GL(n+1, q)$ acts on $X = PG(n, q)$ and so \mathbf{F}_q^X is a module over the group algebra $\mathbf{F}_q G$. The *socle* of a module E , denoted $\text{soc}(E)$, is the sum of all simple submodules or, equivalently, the maximal semisimple submodule. The *radical*, $\text{rad}(E)$, is the intersection of all maximal submodules or, equivalently, the smallest submodule by which the quotient module is semisimple. The higher radicals and socles are defined recursively in the usual way: $\text{soc}^i(E)$ is the full preimage in E of $\text{soc}(E/\text{soc}^{i-1}(E))$ and $\text{rad}^i(E) = \text{rad}(\text{rad}^{i-1}(E))$. Let Y denote the set of hyperplanes in $PG(n, q)$ and let $R = \mathbf{Z}_p[\omega]$ be the extension of the p -adic integers by a primitive $(q-1)$ -th root of unity, so that $R/pR \cong \mathbf{F}_q$. Consider the incidence map $\eta : R^Y \rightarrow R^X$, and let the modules $M_i \subset R^Y$ and $N_i \subset R^X$ be defined as in §2.1, with corresponding submodules $\overline{M}_i \subset \mathbf{F}_q^Y$ and $\overline{N}_i \subset \mathbf{F}_q^X$. Then it can be shown that $\overline{M}_i = \text{rad}^i \mathbf{F}_q^Y$ and $\overline{N}_i = \text{soc}^i \mathbf{F}_q^X$. The radical and socle series of \mathbf{F}_q^X are described in [2]. According to Theorem 3.5 the trace of the matrix M^t is the generating function for the multiplicities of the p -elementary divisors. The multiplicity of p^r is the coefficient a_r of $z^{r(p-1)}$ in this polynomial, which is a sum of t -fold products $\prod_{i=1}^t d_{j_i}$ where $\sum_{i=1}^t p^i d_{j_i} = r(p-1)$. As explained in [2] these t -fold products are the dimensions of simple $\mathbf{F}_q GL(n+1, q)$ -modules, factorized as t -fold twisted tensor products in accordance with Steinberg's tensor product theorem ([21, II/3.17]).

Theorem 3.5 is a special case of a more general result, to be treated in §3.4, from [11], which solves the SNF problem for points versus subspaces of a fixed dimension in $PG(n, q)$.

The cyclic difference sets studied in [12] also arise from multiplicative groups of finite fields, the sums $\chi(B)$ are evaluated using Jacobi sums. Here too, Stickelberger's Theorem applies because of the simple relation between Jacobi and Gauss sums.

Aside from adjacency matrices of graphs, there is also the vertex-edge incidence matrix. A recent paper in this direction is [38], in which the SNF problem for the vertex-edge incidence matrices of a certain class of bipartite graphs is tackled. The approach makes use of Smith's characterization of the invariant factors in terms of the determinantal divisors d_i mentioned in the Introduction. One application of the results is a new calculation of zero-sum mod 2 bipartite Ramsey numbers.

We now turn to a more detailed review of the current state of knowledge about Examples 1.1 and 1.2.

3.3. Subsets of a set. Let S be a finite set of size n and let X_k denote the set of subsets of S of size k . Let $W_{t,k}$ be the inclusion matrix of t -subsets in k -subsets. We think of $W_{t,k}$ as a map $\mathbf{Z}^{X_t} \rightarrow \mathbf{Z}^{X_k}$.

A diagonal form was found in [36].

Theorem 3.6. $W_{t,k}$ has a diagonal form with diagonal entries $\binom{k-i}{t-i}$, each with multiplicity $\binom{n}{i} - \binom{n}{i-1}$, for $0 \leq i \leq t$.

Indispensable ingredients in the proof of these results are the following fundamental identities, which are easily verified.

$$(13) \quad \begin{aligned} W_{i,j} W_{j,t} &= \binom{t-i}{j-i} W_{i,t}, & W_{i,j} \overline{W}_{j,t} &= \binom{n-t-i}{j-i} \overline{W}_{i,t} \\ W_{t,k} &= \sum_{i=0}^t (-1)^i W_{i,t}^T \overline{W}_{i,k}, & \overline{W}_{t,k} &= \sum_{i=0}^t (-1)^i W_{i,t}^T W_{i,k}. \end{aligned}$$

Here, $\overline{W}_{t,k}$ is the disjointness matrix of t -subsets and k -subsets. The matrices $W_{t,k}$ are of course the same as the matrices $\overline{W}_{t,n-k}$ with the columns reordered, since a t -subset is contained in a k -subset if and only if it is disjoint from the complement. Thus, Wilson's formula also solves the SNF problem for the disjointness relation.

The symmetric group S_n acts on S and $W_{t,k}$ is a $\mathbf{Z}S_n$ -module map, so although this action is not used in the original proof, it seems appropriate nevertheless to mention some connections of Theorem 3.6 with the representation theory of S_n . The multiplicities are the dimensions of the simple $\mathbf{Q}S_n$ -submodules of \mathbf{Q}^{X_t} and, over arbitrary fields, of *Specht modules* corresponding to partitions with two parts [20]. The diagonal entries yield the p -rank of $W_{t,k}$ over \mathbf{F}_p , which is helpful in understanding the $\mathbf{F}_p S_n$ -submodule structure of $\mathbf{F}_p^{X_k}$.

In [4], it was shown that with respect to the *Frankl rank* [16] of a subset, there is a canonical choice of $\binom{n}{i} - \binom{n}{i-1}$ rows of $W_{i,k}$, for $i \leq k$, such that the union is a basis of \mathbf{Z}^{X_k} which is a right SNF basis for every $W_{t,k}$, $t \leq k$.

The general case of Example 1.1 is where s , t and k are fixed and a t -subset is incident with a k -subset if and only if their intersection has size s . In the case $t = k \leq n/2$, this defines the $(k-s)$ -th association relation in the *Johnson association scheme* $J(n, k)$. As for the Hamming schemes, the eigenvalues of the association matrices for $J(n, k)$ have been calculated long ago (by Yamamoto et. al. [43] and independently by Ogasawara). However

the SNF problems remain open. A recent paper [37] gives a diagonal form for matrices in the Bose-Mesner Algebra of $J(n, k)$ that satisfy a “primitivity” condition. However, this condition is not satisfied by the association matrices themselves.

Problem 3.7. Solve the SNF problems for the association matrices of the Hamming and Johnson schemes. The answer is known for the relation of maximal distance in both cases. For the Hamming scheme we saw in Example 3.3 that the diagonal entries of a diagonal form were equal, counting multiplicities, to the eigenvalues. This is also true of $J(n, k)$, where the maximal distance relation is the disjointness relation that defines the Kneser graphs $K(n, k)$. The eigenvalues of $K(n, k)$ are the same (up to sign) as the entries of the diagonal form of Theorem 3.6.

3.4. Subspaces of a vector space. We already considered the incidence of points and hyperplanes of $PG(n, q)$ in Example 3.4. Now, we shall look at some further instances of Example 1.2. We shall assume that V is a vector space of dimension $n + 1$ over the field \mathbf{F}_q , with $q = p^t$. For $0 \leq d \leq n + 1$ we denote by \mathcal{L}_d the set of d -dimensional subspaces of V (“ d -subspaces” for short). By analogy with the subsets of a set, we consider for $d \leq e$ the inclusion matrices $A_{d,e}$ of d -subspaces in e -subspaces and the incidence matrices $\overline{A}_{d,e}$ for the relation of zero intersection, whenever $d + e \leq n + 1$.

The most general result obtained so far is for the matrices $A_{1,r}$, where the SNF problem was solved in [11]. As the two statements below show, the Smith group is a product of a cyclic group of order coprime to p (cyclic p' -group for short) and a large p -group, the determination of which is the main work. The statement of this and later results involves a certain partially ordered set. Let \mathcal{H} denote the set of t -tuples of integers $\mathbf{s} = (s_0, \dots, s_{t-1})$ that satisfy, for $0 \leq i \leq t - 1$,

- (1) $1 \leq s_i \leq n$,
- (2) $0 \leq ps_{i+1} - s_i \leq (p - 1)(n + 1)$,

with subscripts read modulo t . First introduced in [17], the set \mathcal{H} was later used in [2] to describe the module structure of $\mathbf{F}_q^{\mathcal{L}_1}$ under the action of $GL(n + 1, q)$. Let

$$(14) \quad \mathcal{H}_\alpha(s) = \left\{ (s_0, \dots, s_{t-1}) \in \mathcal{H} \mid \sum_{i=0}^{t-1} \max\{0, s - s_i\} = \alpha \right\}.$$

To each tuple $\mathbf{s} \in \mathcal{H}$ we associate a number $d(\mathbf{s})$ as follows. For $\mathbf{s} = (s_0, \dots, s_{t-1}) \in \mathcal{H}$ define the integer tuple $\lambda = (\lambda_0, \dots, \lambda_{t-1})$ by

$$\lambda_i = ps_{i+1} - s_i \quad (\text{subscripts mod } t).$$

Finally, set $d(\mathbf{s}) = \prod_{i=0}^{t-1} d_{\lambda_i}$, where d_λ is defined in (12).

Theorem 3.8. *Let $v = |\mathcal{L}_1|$. The invariant factors of $A_{1,r}$ are all p -powers except for the v^{th} invariant, which is a p -power times $(q^r - 1)/(q - 1)$.*

Theorem 3.9. *The p -adic invariant factors of the incidence matrix $A_{1,r}$ between \mathcal{L}_1 and \mathcal{L}_r are p^α , $0 \leq \alpha \leq (r - 1)t$, with multiplicity*

$$e_\alpha = \sum_{\mathbf{s} \in \mathcal{H}_\alpha} d(\mathbf{s}) + \delta(0, \alpha)$$

where

$$(15) \quad \delta(0, \alpha) = \begin{cases} 1, & \text{if } \alpha = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Several themes we have discussed are reflected in the proof of Theorem 3.9. The modules M_i of §2.1 and their relation to the $\mathbf{F}_q \mathrm{GL}(n+1, q)$ -submodule structure of $\mathbf{F}_q^{\mathcal{L}_1}$ play an important role. The space has a basis of monomials and a left SNF basis is constructed by taking Teichmüller lifts of these monomials to a suitable p -adic ring R . Gauss sums and Stickelberger's Theorem then appear, but in a rather different way from equation (11), in computations in the p -adic group ring. A key ingredient is a result of Wan [35], from which one obtains the correct upper bounds for the p -elementary divisors.

In the case of $A_{1,r}$, the p' -part of the Smith group is cyclic. In his Ph.D. thesis [13] Chandler, using results of James [19], has given a diagonal form over the ℓ -adic integers for $\ell \neq p$ for all of the $A_{d,e}$. The result bears a remarkable resemblance to Wilson's diagonal form for subsets, with binomial coefficients replaced by q -binomial coefficients.

Theorem 3.10. *Let $s \leq r$ and $s + r \leq n + 1$. Let ℓ be any prime not dividing q and let \mathbf{Z}_ℓ denote the ℓ -adic integers. Then over \mathbf{Z}_ℓ the matrix $A_{r,s}$ has a diagonal form whose diagonal entries are $\binom{r-i}{s-i}_q$ with multiplicity $\binom{n+1}{i}_q - \binom{n+1}{i-1}_q$.*

Note that whereas, in the case of subsets, $\overline{W}_{t,k}$ is essentially the same as $W_{t,n-k}$ using set complementation, there is no simple relation between $A_{d,e}$ with any $\overline{A}_{r,s}$, except in the case $d = 1$, where $A_{1,e}$ and $\overline{A}_{1,e}$ are complementary. In the case where $r + s = n + 1$, the zero-intersection relation encoded in $\overline{A}_{r,s}$ is an example of an *oppositeness* relation in a spherical Tits building. In general, we know from [7] that for such relations all invariant factors are powers of the natural characteristic p . The first nontrivial example is when $\dim V = 4$ and we consider the relation of zero intersection of 2-dimensional subspaces. Geometrically, we may think of skew lines in projective space. The SNF was determined in [8]. Let $A = \overline{A}_{2,2}$.

Theorem 3.11. *Let $e_i = e_i(A)$ denote the multiplicity of p^i as an elementary divisor of A .*

- (1) $e_i = e_{3t-i}$ for $0 \leq i < t$.
- (2) $e_i = 0$ for $t < i < 2t$, $3t < i < 4t$, and $i > 4t$.
- (3) $\sum_{i=0}^t e_i = q^4 + q^2$.
- (4) $\sum_{i=2t}^{3t} e_i = q^3 + q^2 + q$.
- (5) $e_{4t} = 1$.

Thus we get all the elementary divisor multiplicities once we know t of the numbers e_0, \dots, e_t (or the numbers e_{2t}, \dots, e_{3t}). The next theorem describes these. To state the theorem, we need some notation.

Set

$$[3]^t = \{(s_0, \dots, s_{t-1}) \mid s_i \in \{1, 2, 3\} \text{ for all } i\}$$

and

$$\mathcal{H}(i) = \{(s_0, \dots, s_{t-1}) \in [3]^t \mid \#\{j \mid s_j = 2\} = i\}.$$

In other words, $\mathcal{H}(i)$ consists of the tuples in $[3]^t$ with exactly i twos. To each tuple $\mathbf{s} \in [3]^t$ we associate a number $d(\mathbf{s})$ as follows. For $\mathbf{s} = (s_0, \dots, s_{t-1}) \in [3]^t$ define the integer tuple $\lambda = (\lambda_0, \dots, \lambda_{t-1})$ by

$$\lambda_i = ps_{i+1} - s_i,$$

with the subscripts read mod t . Since $n + 1 = 4$, the integer d_k defined previously in (12) is the coefficient of x^k in the expansion of $(1 + x + \dots + x^{p-1})^4$. Also recall that $d(\mathbf{s}) = \prod_{i=0}^{t-1} d_{\lambda_i}$.

Theorem 3.12. Let $e_i = e_i(A)$ denote the multiplicity of p^i as an elementary divisor of A . Then, for $0 \leq i \leq t$,

$$e_{2t+i} = \sum_{\mathbf{s} \in \mathcal{H}(i)} d(\mathbf{s}).$$

Remark 3.13. When $p = 2$, notice that $d(\mathbf{s}) = 0$ for any tuple \mathbf{s} containing an adjacent 1 and 3 (coordinates read circularly). Thus the sum in Theorem 3.12 is significantly easier to compute in this case.

The proofs involve a combination of the methods already mentioned. The first observation is that the skewness relation defines a strongly regular graph which has integral eigenvalues which are powers of p up to signs. Thus, we may apply Proposition 3.2, which leads to Theorem 3.11. The proof of Theorem 3.12 lies somewhat deeper. The missing elementary divisors can be shown to be the same as for the composite $\overline{A}_{2,1}\overline{A}_{1,2}$. The elementary divisors of $\overline{A}_{2,1}$ and $\overline{A}_{1,2}$ are known from [11]. Then to calculate the SNF of $\overline{A}_{2,1}\overline{A}_{1,2}$ use must be made of the multiplicity-free action of the Singer cycle on $k^{\mathcal{L}^1}$, through Proposition 2.1.

In fact the following more general theorem on composite incidence maps for V of arbitrary dimension is proved in [8], for arbitrary r and s . Let $\mathcal{H}_\beta(r)$ be as defined in (14) and

$$\begin{aligned} \beta\mathcal{H}(r) &= \{(n+1-s_0, \dots, n+1-s_{t-1}) \mid (s_0, \dots, s_{t-1}) \in \mathcal{H}_\beta(r)\} \\ &= \left\{ (s_0, \dots, s_{t-1}) \in \mathcal{H} \mid \sum_{i=0}^{t-1} \max\{0, s_i - (n+1-r)\} = \beta \right\}. \end{aligned}$$

Theorem 3.14. Let $e_i = e_i(\overline{A}_{r,1}\overline{A}_{1,s})$ denote the multiplicity of p^i as a p -adic elementary divisor of $\overline{A}_{r,1}\overline{A}_{1,s}$.

- (1) $e_{t(r+s)} = 1$.
- (2) For $i \neq t(r+s)$,

$$e_i = \sum_{\mathbf{s} \in \Gamma(i)} d(\mathbf{s}),$$

where

$$\Gamma(i) = \bigcup_{\substack{\alpha+\beta=i \\ 0 \leq \alpha \leq t(s-1) \\ 0 \leq \beta \leq t(r-1)}} \beta\mathcal{H}(r) \cap \mathcal{H}_\alpha(s).$$

Summation over an empty set is interpreted to result in 0.

Problem 3.15. Opposite Subspaces Problem. Let $r + s = n + 1$ and let V be an $(n + 1)$ -dimensional vector space over \mathbf{F}_q . Solve the SNF problem for the incidence between the set of r -dimensional subspaces and s -dimensional subspaces, where incidence is defined as zero intersection.

3.5. Spaces with forms. Every question about incidence of subspaces in a vector space prompts analogous questions about vector spaces with bilinear, quadratic or hermitian forms. In these cases, instead of all subspaces one considers a distinguished class, such as totally singular subspaces and their perp spaces with respect to the form. In the case of symplectic forms, Lataille [24] has solved the SNF problem for symplectic vector spaces over a prime field \mathbf{F}_p , as well as computing the p' -factor of the Smith module for the general case over any finite field. In the case of a 6-dimensional vector space with a quadratic form of maximal index, the points of the quadric are the lines of $PG(3, q)$ under the Klein correspondence, so the result of [8] discussed above solves the SNF problem for the relation of (non)collinearity.

If we have a 3-dimensional vector space over \mathbf{F}_{q^2} with a nonsingular Hermitian form, then we may consider the incidence of points and lines of the Hermitian unital. The SNF problem for this case was solved in [18], using results in modular representation theory. In many other cases, there are partial answers, such as the computation of the p -rank, which equals the multiplicity of 1 as a p -elementary divisor. Very little else is known, so it seems reasonable to start in low dimensions. Examples of incidence structures based on low-dimensional vector spaces with forms include the *generalized quadrangles*. (See [26].) These include the classical point line geometries of singular points and totally singular lines in symplectic spaces of (vector) dimension 4, orthogonal spaces of dimension 5 and 6 and in Hermitian spaces of dimensions 4 and 5. One can pose the SNF problem for the point-line incidence or for the collinearity relation.

Problem 3.16. Solve the SNF problem, with respect to one of the incidence relations, for a family of generalized quadrangles. There are no cases for which this problem has yet been solved.

3.6. A word about p -ranks. For many of the incidence relations we have considered, the p -rank, i.e. the rank of the incidence matrix considered over \mathbf{F}_p , has been found, which is the same as computing the multiplicity of 1 as a p -elementary divisor. In the case of subsets, the problem of determining the p -ranks of the i -association matrices of the Johnson scheme $J(n, k)$ for all p would appear to be practically as hard as the full SNF problem. In the case of subspaces the p -ranks of $A_{d,e}$ are still unknown, but the p -ranks of $\bar{A}_{d,e}$ are given by [31]. The p -ranks of some of the generalized quadrangles are known when p is the defining characteristic, and all of the cross-characteristic ranks are known, (from [32] and the references cited there). Also, many of the point-hyperplane p -ranks (in the defining characteristic) can be found in [1]. These are examples of oppositeness relations, or complements of such. For oppositeness relations in the building of a finite group of Lie type of characteristic p it is known ([30]) that the p -ranks are dimensions of irreducible p -modular representations of the group.

The general topic of p -ranks has been studied for a very wide variety of incidence matrices, especially for $p = 2$. One reason for this is that an incidence matrix can be used as a parity-check or generator matrix of a binary code, whose dimension is then given by the 2-rank. The literature is too extensive to summarize here. In the case of designs, many references, examples, applications and open questions are described in [41]. Some recent papers on 2-ranks of incidence structures of certain points and lines in $PG(2, q)$ defined by a conic are [33], [40] and [39].

ACKNOWLEDGEMENTS

I would like to thank Qing Xiang and Josh Ducey for helpful discussions during the preparation of this article.

REFERENCES

1. Ogul Arslan and Peter Sin, *Some simple modules for classical groups and p -ranks of orthogonal and Hermitian geometries*, J. Algebra **327** (2011), 141–169. MR 2746033 (2012d:20092)
2. Matthew Bardoe and Peter Sin, *The permutation modules for $GL(n+1, \mathbf{F}_q)$ acting on $\mathbf{P}^n(\mathbf{F}_q)$ and \mathbf{F}_q^{n-1}* , J. London Math. Soc. (2) **61** (2000), no. 1, 58–80. MR 1745400 (2001f:20103)
3. Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR 1625181 (99d:11092)

4. Thomas Bier, *Remarks on recent formulas of Wilson and Frankl*, European J. Combin. **14** (1993), no. 1, 1–8. MR 1197469 (94b:05006)
5. S. Bittner, X. Guo, and A. Zweber, *Approaches to Rota's Basis Conjecture*, (2012), Report on James Madison University Summer REU 2012.
6. S. C. Black and R. J. List, *On certain abelian groups associated with finite projective geometries*, Geom. Dedicata **33** (1990), no. 1, 13–19. MR 1042620 (90m:05033)
7. Andries E. Brouwer, *The eigenvalues of oppositeness graphs in buildings of spherical type*, Combinatorics and graphs, Contemp. Math., vol. 531, Amer. Math. Soc., Providence, RI, 2010, pp. 1–10. MR 2757785 (2012e:05418)
8. Andries E. Brouwer, Joshua E. Ducey, and Peter Sin, *The elementary divisors of the incidence matrix of skew lines in $PG(3, q)$* , Proc. Amer. Math. Soc. **140** (2012), no. 8, 2561–2573. MR 2910745
9. Andries E. Brouwer and Willem H. Haemers, *Association schemes*, Handbook of combinatorics, Vol. 1, 2, Elsevier, Amsterdam, 1995, pp. 747–771. MR 1373671 (97a:05217)
10. ———, *Spectra of graphs*, Universitext, Springer, New York, 2012. MR 2882891
11. David B. Chandler, Peter Sin, and Qing Xiang, *The invariant factors of the incidence matrices of points and subspaces in $PG(n, q)$ and $AG(n, q)$* , Trans. Amer. Math. Soc. **358** (2006), no. 11, 4935–4957. MR 2231879 (2007c:05041)
12. David B. Chandler and Qing Xiang, *The invariant factors of some cyclic difference sets*, J. Combin. Theory Ser. A **101** (2003), no. 1, 131–146. MR 1953284 (2004c:05034)
13. David Blanchard Chandler, *The Smith normal forms of designs with classical parameters*, ProQuest LLC, Ann Arbor, MI, 2004, Thesis (Ph.D.)—University of Delaware. MR 2706377
14. Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Phillips Research Reports, Suppl., vol. 10, 1973, Thesis, Université Catholique de Louvain.
15. Ronald Evans, Henk D. L. Hollmann, Christian Krattenthaler, and Qing Xiang, *Gauss sums, Jacobi sums, and p -ranks of cyclic difference sets*, J. Combin. Theory Ser. A **87** (1999), no. 1, 74–119. MR 1698269 (2001b:05038)
16. P. Frankl, *Intersection theorems and mod p rank of inclusion matrices*, J. Combin. Theory Ser. A **54** (1990), no. 1, 85–94. MR 1051780 (91b:05006)
17. Noboru Hamada, *The rank of the incidence matrix of points and d -flats in finite geometries*, J. Sci. Hiroshima Univ. Ser. A-I Math. **32** (1968), 381–396. MR 0243903 (39 #5221)
18. Gerhard Hiss, *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups*, Indag. Math. (N.S.) **15** (2004), no. 2, 223–243. MR 2071863 (2005c:20080)
19. G. D. James, *Representations of general linear groups*, London Mathematical Society Lecture Note Series, vol. 94, Cambridge University Press, Cambridge, 1984. MR 776229 (86j:20036)
20. Gordon James and Adalbert Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981, With a foreword by P. M. Cohn, With an introduction by Gilbert de B. Robinson. MR 644144 (83k:20003)
21. Jens Carsten Jantzen, *Representations of algebraic groups*, Pure and Applied Mathematics, vol. 131, Academic Press Inc., Boston, MA, 1987. MR 899071 (89c:20001)
22. Eric S. Lander, *Topics in algebraic coding theory*, 1980, Thesis (D. Phil.)—University of Oxford.
23. ———, *Symmetric designs: an algebraic approach*, London Mathematical Society Lecture Note Series, vol. 74, Cambridge University Press, Cambridge, 1983. MR 697566 (85d:05041)
24. J. M. Lataille, *The elementary divisors of incidence matrices between certain subspaces of a finite symplectic space*, J. Algebra **268** (2003), no. 2, 444–462. MR 2009318 (2004h:20003)
25. F. J. MacWilliams and H. B. Mann, *On the p -rank of the design matrix of a difference set*, Information and Control **12** (1968), 474–488. MR 0242696 (39 #4026)
26. Stanley E. Payne and Joseph A. Thas, *Finite generalized quadrangles*, second ed., EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, 2009. MR 2508121 (2010k:51013)
27. João Filipe Queiró, *Axioms for invariant factors*, Portugal. Math. **54** (1997), no. 3, 263–269. MR 1472161 (98g:15015)
28. Joseph J. Rushanan, *Combinatorial applications of the Smith normal form*, Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), vol. 73, 1990, pp. 249–254. MR 1041855 (90m:15031)
29. Joseph John Rushanan, *Topics in integral matrices and abelian group codes*, ProQuest LLC, Ann Arbor, MI, 1986, Thesis (Ph.D.)—California Institute of Technology. MR 2635072
30. P. Sin, *Oppositeness in buildings and simple modules for finite groups of lie type*, Buildings, Finite Geometries and Groups (2012), 273–286.

31. Peter Sin, *The p -rank of the incidence matrix of intersecting linear subspaces*, Des. Codes Cryptogr. **31** (2004), no. 3, 213–220. MR 2047880 (2004m:05050)
32. Peter Sin and Pham Huu Tiep, *Rank 3 permutation modules of the finite classical groups*, J. Algebra **291** (2005), no. 2, 551–606. MR 2163483 (2006j:20019)
33. Peter Sin, Junhua Wu, and Qing Xiang, *Dimensions of some binary codes arising from a conic in $\text{PG}(2, q)$* , J. Combin. Theory Ser. A **118** (2011), no. 3, 853–878. MR 2763042 (2011m:51016)
34. Henry J. Stephen Smith, *Arithmetical Notes*, Proc. London Math. Soc. **S1-4** (1873), no. 1, 236. MR 1575537
35. Da Qing Wan, *A Chevalley-Warning approach to p -adic estimates of character sums*, Proc. Amer. Math. Soc. **123** (1995), no. 1, 45–54. MR 1215208 (95c:11147)
36. Richard M. Wilson, *A diagonal form for the incidence matrices of t -subsets vs. k -subsets*, European J. Combin. **11** (1990), no. 6, 609–615. MR 1078717 (91i:05010)
37. Richard M. Wilson and Tony W. H. Wong, *Diagonal forms of incidence matrices associated with t -uniform hypergraphs*, (2012), Preprint.
38. Tony W. H. Wong, *Diagonal forms and zero sum (mod 2) bipartite ramsey numbers*, (2012), Preprint.
39. Junhua Wu, *Geometric structures and linear codes related to conics in classical projective planes of odd orders*, ProQuest LLC, Ann Arbor, MI, 2008, Thesis (Ph.D.)—University of Delaware. MR 2712639
40. ———, *Some p -ranks related to a conic in $\text{PG}(2, q)$* , J. Combin. Des. **18** (2010), no. 3, 224–236. MR 2656395 (2011f:51008)
41. Qing Xiang, *Recent results on p -ranks and Smith normal forms of some 2 -(v, k, λ) designs*, Coding theory and quantum computing, Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 53–67. MR 2170799 (2006h:05035)
42. K. Yamamoto, *On congruences arising from relative Gauss sums*, Number theory and combinatorics. Japan 1984 (Tokyo, Okayama and Kyoto, 1984), World Sci. Publishing, Singapore, 1985, pp. 423–446. MR 827799 (87g:11164)
43. Sumiyasu Yamamoto, Yoshio Fujii, and Noboru Hamada, *Composition of some series of association algebras*, J. Sci. Hiroshima Univ. Ser. A-I Math. **29** (1965), 181–215. MR 0211886 (35 #2761)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, P. O. BOX 118105, GAINESVILLE FL 32611, USA